UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/868,387 | 09/10/2002 | Harri Vatanen | 2132-47PCON | 8959 |

7590 10/28/2008

Lance J Lieberman
Cohen Pontani Lieberman & Pavane
Suite 1210
551 Fifth Avenue
New York, NY 10176

| EXAMINER | |
|---|---|
| TRUVAN, LEYNNA THANH | |
| ART UNIT | PAPER NUMBER |
| 2435 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/28/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/868,387 | VATANEN, HARRI | |
| | Examiner | Art Unit | |
| | Leynna T. Truvan | 2435 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *11 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date. _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____

## DETAILED ACTION

**1.** Claims 1-24 are pending.

### *Response to Arguments*

**2.** Applicant's arguments filed 7/11/2008 have been fully considered but they are not persuasive.

Regarding the argument on pg.10-11, that Nishioka does not teach or suggest a payment machine that generates a document that is sent to the mobile station and computes a hash with the document, and receives the signed document from the user and verifies the authenticity of the document by checking the signed hash. Examiner notes that independent claim 1 does not recite the payment machine generate a document. As for independent claim 13, recite means connected to the payment machine for the generation of the material to be signed. It broadly suggests the "means" is for generation of the material and not the payment machine because it does not claim the means for the payment machine for generation. Rather the payment machine is merely connected to means for generation of the material. Thus, the claimed invention does not recite or suggest a payment machine that generates a document. Innuendo, Nishioka does include means connected to the payment machine for the generation of the material in the producing unit for producing a document (col.9, lines 16-20 and 37-38).

As for sending the document which is the claimed material to the mobile station is disclosed by Nishioka. Nishioka includes a smart card input/output unit for transmitting/receiving data to/from the smart card (col.9, lines 34-36 and col.10, lines 65-67). Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50).

According to arguments on pg.11, that Nishioka does not teach or suggest verifying the authenticity of the document by checking the hash. As established in the last office action that Nishioka did not go into details of signing the material and verifying the digital signature in the payment machine. Therefore, Anderson is brought forth to suggest that it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine with Nishioka to teach a method and system of signing the document and verifying the digital signature in the payment machine because digital signature insures that the electronic document is authentic that has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11) and for the payer (payment machine) to validate the signature verifies the payee's signature transaction (col.23, lines 39-41 and col.24, lines 63-67) where verifier trust the association between the signer and the public key used to verify the signature on the document, thus authenticates the payee (col.26, line 46 – col.27, line 12). Thus, the Nishioka and Anderson combination suggests the signature card (mobile station) signing both the hash and document and

then verifying the signature at the payer (payment machine) to verify and authenticate the authenticity as claimed.

As for argument on pg.11 (2nd paragraph) – pg.12, that Anderson does not teach or suggest computing in the payment machine, a first hash code for the material to be signed. Anderson's payee is referring to the claimed payment machine and to user site apparatus of Nishioka. Examiner notes that Anderson is not relied on as the primary art that teach or suggest computing in the payment machine, a first hash code for the material to be signed. Applicant acknowledges the payee receives and validates the signature. Thus, obviously suggests Anderson includes the method or scheme of a payment machine verifying the authenticity of the signed and transferred material where another one device/machine (i.e. mobile station) the hash and so forth discussed above. Anderson suggests the claimed verifying, in the payment machine, the authenticity of the signed and transferred material (Anderson col.26, line 46 – col.27, line 12) by comparing the signed hash code with the first hash code computed from the material before signature (Anderson-col.23, lines 39-41 and col.24, lines 63-67). The Anderson method that allows one device/machine (i.e. mobile station) to sign the material and have another device/machine verify the authenticity is obvious that it does not matter or limited to a specific device a payee, payer, or mobile station. Whereas, Anderson's signature scheme allows two different device/machine to interact with each other for verification to a material's authenticity so that this method can be used in any system as long as there is one device/machine signs the material and have another device/machine verify the authenticity.. Thus, would be obvious for a person of ordinary

skills in the art to apply and combine to Nishioka's teaching in order to insure that the electronic document is authentic that has not been tampered with (Anderson-col.20, lines 22-32 and col.21, lines 10-11) and thus authenticates the trust (col.26, line 46 – col.27, line 12).

Claim 13 recites similar limitations and thus is also rejected in view of Nishioka and Anderson combination.

All other dependent claims are also rejected by virtue of their dependency.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**3. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nishioka, et al. (US 5,754,656), and further in view of Anderson, et al. (US 6,209,095).**

**As per claim 1:**

Nishioka, et al. teaches a method for digitally signing an electronic form in a secure manner by a mobile station said method comprising the steps of:

computing, in a payment machine **[col.2, lines 35-48 and col.9, lines 2-5]**, a first hash code for the material **[col.13, lines 21-23 and col.21, lines 58-61]** to be signed, the material to be signed including the form, an identifier of the form, shared information, and /or information in essential fields of the form; **[col.21, lines 6-14 and 62-65; the term essential is relative to what is considered essential or its limit of how essential is considered essential for the fields of the form. Thus, information in essential fields of the form can broadly be given as data such a key, a hash value, product names, prices of the products, or kinds of products such that these information are essential to identify the product the user is looking to purchase or essential to verify the signature so that the material is what the material is said to be.]**

transferring the material **[col.10, line 66 – col.11, line 1]** to be signed and the first hash code in a payment machine to the mobile station, **[col.13, lines 21-26 and col.22, lines 3-5; Nishioka discloses a user site apparatus as the claimed payment machine and the smart card refers to the claimed mobile station (explained further below). ]**

digitally signing, using the mobile station, [*the material*] and the first hash code transferred to the mobile station; and **[col.13, lines 35-40 and col.22, lines 7-8]**

*[verifying, in the payment machine, the authenticity of the signed and transferred material (Anderson col.26, line 46 – col.27, line 12) by comparing the signed hash code with the first hash code computed from the material before signature (Anderson-col.23, lines 39-41 and col.24, lines 63-67).]*

Nishioka discloses an electronic shopping system that includes a user site apparatus corresponds to a terminal or the like (col.9, lines 15-20) which includes a smart card input/output unit for receiving the smart card and transmitting/receiving data to/from the smart card (col.9, lines 1-5 and 34-36). Nishioka discloses an electronic shopping system where the user can receive product information to be purchased and where the user site apparatus sends credit card information and the sum of purchased products (col.10, lines 50-52). Thus, Nishioka obviously suggests purchasing and payment information and therefore the user site apparatus is obviously the claimed payment machine. The claimed material can broadly be interpreted as data or information that pertains to a document where document is outputted to the smart card (col.10, line 66 – col.11, line 1). The smart card is the claimed mobile station. Further, Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50). Although, Nishioka discloses the mobile station signing the hash and then verifying the signed hash by comparing the signed hash code with the first hash code from the material before signature, but did not go into details of signing the material and verifying the digital signature in the payment machine.

Anderson discloses the invention of an all-electronic payments (col.14, lines 25-28) and a computer-based method for creating a signed electronic document (col.10, lines 36-38) where the invention includes a portable electronic device (i.e.

PCMCIA/smart card or signature cards) to provide greater security for a financial transaction that is able to calculate and verify digital signatures (col.30, lines 41-58). The card always keeping the private key internal to the processor and memory on the card where the document to be signed uses the private key to compute the signature (col.27, lines 26-29). Anderson discloses the signature cards can be used to better secure the private keys and greatly reduce the need for diligence and against attacks through network connections by computer hackers (col.27, lines 40-53). The use of digital signatures make the electronic documents trusted and secure that will provide greater security and reduced fraud losses for all parties in the transaction process (col.15, lines 6-18). Anderson also discusses a method of attaching a document to a related electronic document by forming a cryptographic hash of the document and appending the hash to the electronic document and signing the hash (col.13, lines 60-67 and col.21, lines 30-41). The signing of electronic documents can employ a public key cryptographic signature and hash algorithm to provide security attributes wherein the FSML signature mechanism allows documents to be combined, or added to, without lost of security attributes (col.19, lines 8-12). Anderson discloses the blocks making up the electronic document can be protected from tampering and all blocks need to be authenticated are assigned a digital signature and digitally signing the hash such that the digital signature of the hash can be incorporated into the block for the contents of the block can be signed (col.20, lines 7-9 and col.21, lines 17-22). Thus, Anderson's technique verifies that all the blocks that are bound together are present and have not been tampered with such that the integrity of the entire document is verifiable (col.20,

lines 22-32 and 43-47). In addition, Anderson discloses the payer as the payment machine validates the payee's (mobile station or card) signature by using the payer's public key to verify the payee's signature transaction and thus authenticates the payee (col.23, lines 39-41 and col.24, lines 63-67). Anderson discloses the signature are produced by signer's private key and the message to be signed as inputs to the public key signature algorithm such that to verify the signature can be verified by knowing the signer's public key where the verifier trust the association between the signer and the public key used to verify the signature on the document (col.26, line 46 – col.27, line 12). Therefore, Anderson suggests the signature card (mobile station) signing both the hash and document and then verifying the signature at the payer (payment machine) to verify and authenticate the authenticity as claimed.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine Nishioka with Anderson to teach signing the document and verifying the digital signature in the payment machine because digital signature insures that the electronic document is authentic that has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11) and for the payer (payment machine) to validate the signature verifies the payee's signature transaction (col.23, lines 39-41 and col.24, lines 63-67) where verifier trust the association between the signer and the public key used to verify the signature on the document, thus authenticates the payee (col.26, line 46 – col.27, line 12).

**As per claim 2:** **See Nishioka on col.22, lines 3-5;** discussing the first hash code is added to the material to be transferred to the mobile station.

**As per claim 3:** **See Nishioka on col.21, lines 6-10 and 62-65 and Anderson on col.20, lines 29-32 and col.21, lines 10-11;** discussing the material to be signed is generated from an identifier of the form and information in the essential fields of the form.

**As per claim 4:** **See Nishioka on col.21, lines 58-61;** discussing computing the first hash code from the material to be signed before the material is transferred into the mobile station.

**As per claim 5:** **See Anderson on col.20, lines 29-46 and col.21, lines 10-11;** discussing the material is transferred from a payment machine to the mobile station **(Nishioka on col.16, lines 26-30)** for signature is also transferred from the payment machine to a second party **(Nishioka on col.15, lines 45-51 and col.18, lines 36-45)** and the signed material is transferred from the mobile station to the second party **(Nishioka on col.13, lines 41-45)**, whereupon the second party performs the step of verifying the authenticity of the signature. **(Nishioka on col.14, lines 22-24)**

**As per claim 6:** **See Nishioka on col.21, lines 3-19;** discussing the material is encrypted before being transferred between the mobile station and the second party and the encrypted material is decrypted before the signing of the material and before the verification of authenticity.

Nishioka discloses deciphering the document P, calculates the hash value and then confirming the signature and as a result document P is carried out (**Nishioka on col.14, lines 40-49).** This suggests the document P is not signed before encryption and

decryption of the encrypted material because document P is carried out as a result to a legality of the digital signature from the calculated hash value.

**As per claim 7: See Nishioka on col.21, lines 6-14 and 62-65 and col.22, lines 40-42;** discussing the form is generated using a pre-agreed form template provided with an identifier, the information the essential fields of the form being filled in the form template before it is transferred to the mobile station.

**As per claim 8: See Nishioka on col.21, lines 59-61;** discussing the hash code is generated using a hash function.

**As per claim 9: See Nishioka on col.22, lines 8-10 and 57;** discussing the signature and/or encryption of the message is implemented using a public and private key method.

**As per claim 10: See Nishioka on col.13, lines 3-8 and Anderson on col.20, lines 29-32 and col.21, lines 10-11;** discussing the material or part of the material is presented on the display in the mobile station before the material is signed.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

**As per claim 11: See Nishioka on col.12, lines 27-28;** discussing wherein the mobile station is started in signature mode before the transfer of the material into the mobile station.

**As per claim 12: See Nishioka on col.22, lines 1-2 and Anderson on col.31, lines 28-32;** discussing the material is stamped with a the stamp, and a transaction of the signing of the material is filed after the signature has been authenticated.

Nishioka discloses deciphering the document P, calculates the hash value and then confirming the signature and as a result document P is carried out (**Nishioka on col.14, lines 40-49).** This suggests the document P is not signed until the signature has been authenticated because document P is carried out as a result to a legality of the digital signature.

**As per claim 13:**

Nishioka, et al. teaches a system for digitally signing an electronic form in a secure manner by a mobile station said system comprising:

a payment machine; **[col.2, lines 35-48 and col.9, lines 2-5; discusses the user site apparatus is in the form of a payment machine is a terminal for the user to insert the smart card into (col.9, lines 16-28) that communicates to the retail store apparatus where this payment apparatus issues commands for purchasing the desired products and thus the user site apparatus is where payment takes place in order to complete the purchase via the retail store apparatus (col.9, lines 3-5 and 10-13).]**

means connected to the payment machine for the generation of the material **[col.10, line 66 – col.11, line 1]** said material comprising a form, its identifier, shared data, and/or information in essential fields of the form; and **[col.21, lines 6-14 and 62-65 and col.22, lines 40-42; the term essential is relative to what is considered**

**essential or its limit of how essential is considered essential for the fields of the form. Thus, information in essential fields of the form can broadly be given as data such a key, a hash value, product names, prices of the products, or kinds of products such that these information are essential to identify the product the user is looking to purchase or essential to verify the signature so that the material is what the material is said to be.]**

means connected to the payment machine for the transfer of the material into the mobile station, wherein **[col.9, lines 34-50 and col.13, lines 24-26 and col.22, lines 3-5; discusses the smart card in the form of the mobile station where the smart card is mobile and is inserted in by a user, that can receive/transmit data, encrypt/decrypt unit, and a digital signature unit. (col.9, lines 55-56 and col.22, lines 6-7).]**

the payment machine comprises means for computing a first hash code from the material to be signed **[col.13, lines 35-40 and col.22, lines 7-8]** and means for transfer of the first hash code into the mobile station; **[col.13, lines 21-26 and col.22, lines 3-5]**

the mobile station, comprises signing means for the signing of [*the material*] and the first hash code transferred to the mobile station; and **[col.13, lines 35-40 and col.22, lines 7-8]**

*[the payment machine comprises means for verifying the authenticity of the signed and transferred material (Anderson col.26, line 46 – col.27, line 12) by comparing the signed hash code with the hash code computed from the material before signature (Anderson-col.23, lines 39-41 and col.24, lines 63-67).]*

Nishioka discloses an electronic shopping system that includes a user site apparatus corresponds to a terminal or the like (col.9, lines 15-20) which includes a smart card input/output unit for receiving the smart card and transmitting/receiving data to/from the smart card (col.9, lines 1-5 and 34-36). Nishioka discloses an electronic shopping system where the user can receive product information to be purchased and where the user site apparatus sends credit card information and the sum of purchased products (col.10, lines 50-52). Thus, Nishioka obviously suggests purchasing and payment information and therefore the user site apparatus is obviously the claimed payment machine. The claimed material can broadly be interpreted as data or information that pertains to a document where document is outputted to the smart card (col.10, line 66 – col.11, line 1). The smart card is the claimed mobile station. Further, Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50). Although, Nishioka discloses the mobile station signing the hash and then verifying the signed hash by comparing the signed hash code with the first hash code from the material before signature, but did not go into details of signing the material and verifying the digital signature in the payment machine.

Anderson discloses the invention of an all-electronic payments (col.14, lines 25-28) and a computer-based method for creating a signed electronic document (col.10, lines 36-38) where the invention includes a portable electronic device (i.e.

PCMCIA/smart card or signature cards) to provide greater security for a financial transaction that is able to calculate and verify digital signatures (col.30, lines 41-58). The card always keeping the private key internal to the processor and memory on the card where the document to be signed uses the private key to compute the signature (col.27, lines 26-29). Anderson discloses the signature cards can be used to better secure the private keys and greatly reduce the need for diligence and against attacks through network connections by computer hackers (col.27, lines 40-53). The use of digital signatures make the electronic documents trusted and secure that will provide greater security and reduced fraud losses for all parties in the transaction process (col.15, lines 6-18). Anderson also discusses a method of attaching a document to a related electronic document by forming a cryptographic hash of the document and appending the hash to the electronic document and signing the hash (col.13, lines 60-67 and col.21, lines 30-41). The signing of electronic documents can employ a public key cryptographic signature and hash algorithm to provide security attributes wherein the FSML signature mechanism allows documents to be combined, or added to, without lost of security attributes (col.19, lines 8-12). Anderson discloses the blocks making up the electronic document can be protected from tampering and all blocks need to be authenticated are assigned a digital signature and digitally signing the hash such that the digital signature of the hash can be incorporated into the block for the contents of the block can be signed (col.20, lines 7-9 and col.21, lines 17-22). Thus, Anderson's technique verifies that all the blocks that are bound together are present and have not been tampered with such that the integrity of the entire document is verifiable (col.20,

lines 22-32 and 43-47). In addition, Anderson discloses the payer as the payment machine validates the payee's (mobile station or card) signature by using the payer's public key to verify the payee's signature transaction and thus authenticates the payee (col.23, lines 39-41 and col.24, lines 63-67). Anderson discloses the signature are produced by signer's private key and the message to be signed as inputs to the public key signature algorithm such that to verify the signature can be verified by knowing the signer's public key where the verifier trust the association between the signer and the public key used to verify the signature on the document (col.26, line 46 – col.27, line 12). Therefore, Anderson suggests the signature card (mobile station) signing both the hash and document and then verifying the signature at the payer (payment machine) to verify and authenticate the authenticity as claimed.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine Nishioka with Anderson to teach signing the document and verifying the digital signature in the payment machine because digital signature insures that the electronic document is authentic that has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11) and for the payer (payment machine) to validate the signature verifies the payee's signature transaction (col.23, lines 39-41 and col.24, lines 63-67) where verifier trust the association between the signer and the public key used to verify the signature on the document, thus authenticates the payee (col.26, line 46 – col.27, line 12).

**As per claim 14: See Nishioka on col.20, lines 54-57 and col.21, lines 4-5 and 18-19;** discussing a server connected to the payment machine and the mobile station and controlled by a second party, and the mobile station comprises means for encrypting the signed material.

**As per claim 15: See Nishioka on col.22, lines 49-55 and Anderson-col.23, lines 39-41 and col.24, lines 63-67;** discussing the server comprises means for the verification of authenticity of the digital signature.

**As per claim 16: See Nishioka on col.13, lines 3-8 and Anderson col.21, lines 6-10 and 62-65 and col.22, lines 40-42;** discussing the mobile station comprises means for presenting the material or part of the material on the display of it in the mobile station before the signing of the material.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

**As per claim 17: See Nishioka on col.22, lines 1-2 and Anderson on col.31, lines 28-32;** discussing means for stamping the material with a time stamp, and means for filing the transaction of signing of the material after the signature has been authenticated.

Nishioka discloses deciphering the document P, calculates the hash value and then confirming the signature and as a result document P is carried out **(Nishioka on col.14, lines 40-49).** This suggest the document P is not signed until the signature has been authenticated because

**As per claim 18: See Nishioka on col.13, lines 3-8 and Anderson on col.20, lines 29-32 and col.21, lines 10-11;** discussing the method as defined in claim 1, wherein the mobile station has a display configured to present to a user of the mobile station at least a portion of the material.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

**As per claim 19: See Nishioka on col.13, lines 3-8 and Anderson on col.20, lines 29-32 and col.21, lines 10-11;** discussing the method as defined in claim 13, wherein the mobile station has a display configured to present to a user of the mobile station at least a portion of the material.

Nishioka discloses information being displayed on a display device. Thereafter on col.13, lines 9-39, obviously supports material is signed after the material is presented on the display.

**As per claim 20: See Anderson on col.20, lines 16-31 and col.27, lines 25-30;** discussing method as defined in claim 1, wherein said step of transferring comprises transferring the material to be signed and the first hash code directly from the payment machine to the mobile station using only a wireless transmission.

**As per claim 21: See Anderson on col.38, lines 15-16;** discussing the as defined in claim 20, wherein the wireless transmission used one of Bluetooth and infrared technology.

**As per claim 22: See Anderson on col.20, lines 16-31 and col.27, lines 25-30;** discussing system as defined in claim 13, wherein the means connected to the payment machine for the transfer of the material into the mobile station includes a wireless transmission means.

**As per claim 23: See Anderson on col.38, lines 15-16;** discussing system as defined in claim 22, wherein the wireless transmission means uses one of Bluetooth and infrared technology.

**As per claim 24:**

Nishioka, et al. teaches a method for digitally signing an electronic form in a payment transaction between in a secure manner by a payer using a mobile station, said method comprising the steps of:

computing, in a local payment machine of the payee **[col.2, lines 35-48 and col.9, lines 2-5; discusses the user site apparatus is in the form of a payment machine is a terminal for the user to insert the smart card into (col.9, lines 16-28) that communicates to the retail store apparatus where this payment apparatus issues commands for purchasing the desired products and thus the user site apparatus is where payment takes place in order to complete the purchase via the retail store apparatus (col.9, lines 3-5 and 10-13).]**, a first hash code for the material to be signed **[col.10, line 66 – col.11, line 1]**, the material to be signed including the form, an identifier of the form, shared information, and/or information in essential fields of the form; **[col.21, lines 6-14 and 62-65 and col.22, lines 40-42; the term essential is relative to what is considered essential or its limit of how essential is considered essential for the fields of the form. Thus,**

**information in essential fields of the form can broadly be given as data such a key, a hash value, product names, prices of the products, or kinds of products such that these information are essential to identify the product the user is looking to purchase or essential to verify the signature so that the material is what the material is said to be.]**

transferring, from the payment machine to the mobile station of the payer, the material to be signed and the first hash code, the mobile station being configured for wireless communication in a wireless communication network; **[col.9, lines 34-50 and col.13, lines 24-26 and col.22, lines 3-5; discusses the smart card in the form of the mobile station where the smart card is mobile and is inserted in by a user, that can receive/transmit data, encrypt/decrypt unit, and a digital signature unit. (col.9, lines 55-56 and col.22, lines 6-7).]**

the payment machine comprises means for computing a first hash code from the material to be signed **[col.13, lines 35-40 and col.22, lines 7-8]** and means for transfer of the first hash code into the mobile station; **[col.13, lines 21-26 and col.22, lines 3-5]**

digitally signing, by the payer using the mobile station, [*the material*] and the first hash code transferred to the mobile station; and **[col.13, lines 35-40 and col.22, lines 7-8]**

*[verifying, in the payment machine, the authenticity of the signed and transferred material (Anderson col.26, line 46 – col.27, line 12) by comparing the signed hash code with the hash code computed from the material before signature (Anderson-col.23, lines 39-41 and col.24, lines 63-67).]*

Nishioka discloses an electronic shopping system that includes a user site apparatus corresponds to a terminal or the like (col.9, lines 15-20) which includes a

smart card input/output unit for receiving the smart card and transmitting/receiving data to/from the smart card (col.9, lines 1-5 and 34-36). Nishioka discloses an electronic shopping system where the user can receive product information to be purchased and where the user site apparatus sends credit card information and the sum of purchased products (col.10, lines 50-52). Thus, Nishioka obviously suggests purchasing and payment information and therefore the user site apparatus is obviously the claimed payment machine. The claimed material can broadly be interpreted as data or information that pertains to a document where document is outputted to the smart card (col.10, line 66 – col.11, line 1). The smart card is the claimed mobile station. Further, Nishioka discloses a hash calculator for calculating the hash value of a part in the document and supplies the hash to the smart card (col.12, lines 38-39 and col.13, lines 20-25). Thus, Nishioka suggests the document and the hash value are transferred to the smart card where a signature is calculated (col.13, lines 35-37 and col.19, lines 29-50). Although, Nishioka discloses the mobile station signing the hash and then verifying the signed hash by comparing the signed hash code with the first hash code from the material before signature, but did not go into details of signing the material and verifying the digital signature in the payment machine.

Anderson discloses the invention of an all-electronic payments (col.14, lines 25-28) and a computer-based method for creating a signed electronic document (col.10, lines 36-38) where the invention includes a portable electronic device (i.e. PCMCIA/smart card or signature cards) to provide greater security for a financial transaction that is able to calculate and verify digital signatures (col.30, lines 41-58).

The card always keeping the private key internal to the processor and memory on the card where the document to be signed uses the private key to compute the signature (col.27, lines 26-29). Anderson discloses the signature cards can be used to better secure the private keys and greatly reduce the need for diligence and against attacks through network connections by computer hackers (col.27, lines 40-53). The use of digital signatures make the electronic documents trusted and secure that will provide greater security and reduced fraud losses for all parties in the transaction process (col.15, lines 6-18). Anderson also discusses a method of attaching a document to a related electronic document by forming a cryptographic hash of the document and appending the hash to the electronic document and signing the hash (col.13, lines 60-67 and col.21, lines 30-41). The signing of electronic documents can employ a public key cryptographic signature and hash algorithm to provide security attributes wherein the FSML signature mechanism allows documents to be combined, or added to, without lost of security attributes (col.19, lines 8-12). Anderson discloses the blocks making up the electronic document can be protected from tampering and all blocks need to be authenticated are assigned a digital signature and digitally signing the hash such that the digital signature of the hash can be incorporated into the block for the contents of the block can be signed (col.20, lines 7-9 and col.21, lines 17-22). Thus, Anderson's technique verifies that all the blocks that are bound together are present and have not been tampered with such that the integrity of the entire document is verifiable (col.20, lines 22-32 and 43-47). In addition, Anderson discloses the payer as the payment machine validates the payee's (mobile station or card) signature by using the payer's

public key to verify the payee's signature transaction and thus authenticates the payee (col.23, lines 39-41 and col.24, lines 63-67). Anderson discloses the signature are produced by signer's private key and the message to be signed as inputs to the public key signature algorithm such that to verify the signature can be verified by knowing the signer's public key where the verifier trust the association between the signer and the public key used to verify the signature on the document (col.26, line 46 – col.27, line 12). Therefore, Anderson suggests the signature card (mobile station) signing both the hash and document and then verifying the signature at the payer (payment machine) to verify and authenticate the authenticity as claimed.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine Nishioka with Anderson to teach signing the document and verifying the digital signature in the payment machine because digital signature insures that the electronic document is authentic that has not been tampered with (col.20, lines 22-32 and col.21, lines 10-11) and for the payer (payment machine) to validate the signature verifies the payee's signature transaction (col.23, lines 39-41 and col.24, lines 63-67) where verifier trust the association between the signer and the public key used to verify the signature on the document, thus authenticates the payee (col.26, line 46 – col.27, line 12).

***Conclusion***

**4. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2431